

1 Michael A. Sherman (SBN 94783)
masherman@stubbsalderton.com
2 Jeffrey F. Gersh (SBN 87124)
jgersh@stubbsalderton.com
3 Sandeep Seth (SBN 195914)
sseth@stubbsalderton.com
4 Wesley W. Monroe (SBN 149211)
wmonroe@stubbsalderton.com
5 Stanley H. Thompson, Jr. (SBN 198825)
sthompson@stubbsalderton.com
6 Viviana Boero Hedrick (SBN 239359)
vhedrick@stubbsalderton.com
7 STUBBS, ALDERTON & MARKILES, LLP
15260 Ventura Blvd., 20th Floor
8 Sherman Oaks, CA 91403
Telephone: (818) 444-4500
9 Facsimile: (818) 444-4520

Attorneys for Plaintiffs
[Additional Attorneys listed
below]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

PERSONALWEB TECHNOLOGIES, LLC, a Texas limited liability company, and LEVEL 3 COMMUNICATIONS, LLC, a Delaware limited liability company,

Plaintiffs,

CASE NO.:

COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

5

TWITCH INTERACTIVE, INC., a Delaware corporation,

Defendant.

1 Plaintiff PersonalWeb Technologies, LLC (“Plaintiff” or “PersonalWeb”) files this Complaint
2 for patent infringement against Defendant Twitch Interactive, Inc. (“Defendant”). Plaintiff
3 PersonalWeb Technologies, LLC alleges:

4

5 **PRELIMINARY STATEMENT**

6 1. PersonalWeb and Level 3 Communications, LLC (“Level 3”) are parties to an
7 agreement between Kinetech, Inc. and Digital Island, Inc. dated September 1, 2000 (the “Agreement”).
8 Pursuant to the Agreement, PersonalWeb and Level 3 each own a fifty percent (50%) undivided
9 interest in and to the patents at issue in this action: U.S. Patent Nos. 6,928,442, 7,802,310, 7,945,544,
10 and 8,099,420 (“Patents-in-Suit”). Level 3 has joined in this Complaint pursuant to its contractual
11 obligations under the Agreement, at the request of PersonalWeb.

12 2. Pursuant to the Agreement, Level 3 has, among other rights, certain defined rights to
13 use, practice, license, sublicense and enforce and/or litigate the Patents-in-Suit in connection with a
14 particular field of use (“Level 3 Exclusive Field”). Pursuant to the Agreement PersonalWeb has,
15 among other rights, certain defined rights to use, practice, license, sublicense, enforce and/or litigate
16 the Patents-in-Suit in fields other than the Level 3 Exclusive Field (the “PersonalWeb Patent Field”).

17 3. All infringement allegations, statements describing PersonalWeb, statements
18 describing any Defendant (or any Defendant’s products) and any statements made regarding
19 jurisdiction and venue are made by PersonalWeb alone, and not by Level 3. PersonalWeb alleges that
20 the infringements at issue in this case all occur within, and are limited to, the PersonalWeb Patent
21 Field. Accordingly, PersonalWeb has not provided notice to Level 3—under Section 6.4.1 of the
22 Agreement or otherwise—that PersonalWeb desires to bring suit in the Level 3 Exclusive Field in its
23 own name on its own behalf or that PersonalWeb knows or suspects that Defendant is infringing or
24 has infringed any of Level 3’s rights in the patents.

THE PARTIES

4. Plaintiff PersonalWeb Technologies, LLC is a limited liability company duly organized and existing under the laws of Texas with its principal place of business at 112 E. Line Street, Suite 204, Tyler, TX 75702.

5. Plaintiff Level 3 Communications, LLC is a limited liability company organized under the laws of Delaware with its principal place of business at 100 CenturyLink Drive, Monroe, Louisiana, 71203.

6. PersonalWeb's infringement claims asserted in this case are asserted by PersonalWeb and all fall outside the Level 3 Exclusive Field. Level 3 is currently not asserting patent infringement in this case in the Level 3 Exclusive Field against any Defendant.

7. Defendant Twitch Interactive, Inc. is, upon information and belief, a Delaware corporation having a principal place of business and regular and established place of business at 225 Bush Street, 6th Floor, San Francisco, California 94104.

JURISDICTION AND VENUE

8. The court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a) because this action arises under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*

9. Venue is proper in this federal district pursuant to 28 U.S.C. §§ 1391(b)–(c) and 1400(b) because Defendant is incorporated in the state of Delaware and, on information and belief, has a regular and established place of business in this District and has committed acts of infringement in this District.

10. This court has personal jurisdiction over Defendant because, in addition to the allegations in above paragraphs, on information and belief, Defendant is domiciled in this District. Further, on information and belief, Defendant purposefully directed activities at residents of California, the claims herein arise out of and relate to those activities, and assertion of personal jurisdiction over Defendant would be fair.

PERSONALWEB BACKGROUND

11. The Patents-in-Suit cover fundamental aspects of cloud computing, including the identification of files or data and the efficient retrieval thereof in a manner which reduces bandwidth transmission and storage requirements.

12. The ability to reliably identify and access specific data is essential to any computer system or network. On a single computer or within a small network, the task is relatively easy: simply name the file, identify it by that name and its stored location on the computer or within the network, and access it by name and location. Early operating systems facilitated this approach with standardized naming conventions, storage device identifiers, and folder structures.

13. Ronald Lachman and David Farber, the inventors of the Patents-in-Suit, recognized that the conventional approach for naming, locating, and accessing data in computer networks could not keep pace with ever-expanding, global data processing networks. New distributed storage systems use files that are stored across different devices in dispersed geographic locations. These different locations could use dissimilar conventions for identifying storage devices and data partitions. Likewise, different users could give identical names to different files or parts of files—or unknowingly give different names to identical files. No solution existed to ensure that identical file names referred to the same data, and conversely, that different file names referred to different data. As a result, expanding networks could not only become clogged with duplicate data, they also made locating and controlling access to stored data more difficult.

14. Lachman and Farber developed a solution: replacing conventional naming and storing conventions with system-wide “substantially unique,” content-based identifiers. Their approach assigned substantially unique identifiers to “data items” of any type: “the contents of a file, a portion of a file, a page in memory, an object in an object-oriented program, a digital message, a digital scanned image, a part of a video or audio signal, or any other entity which can be represented by a sequence of bits.” Applied system-wide, this invention would permit any data item to be stored, located, managed, synchronized, and accessed using its content-based identifier.

15. To create a substantially unique, content-based identifier, Lachman and Farber turned to cryptography. Cryptographic hash functions, including MD4, MD5, and SHA, had been used in

1 computer systems to verify the integrity of retrieved data—a so-called “checksum.” Lachman and
2 Farber recognized that these same hash functions could be devoted to a vital new purpose: if a
3 cryptographic hash function was applied to a sequence of bits (a “data item”), it would produce a
4 substantially unique result value, one that: (1) virtually guarantees a different result value if the data
5 item is changed; (2) is computationally difficult to reproduce with a different sequence of bits; and
6 (3) cannot be used to recreate the original sequence of bits.

7 16. These cryptographic hash functions would thus assign any sequence of bits, based on
8 content alone, with a substantially unique identifier. Lachman and Farber estimated that the odds of
9 these hash functions producing the same identifier for two different sequences of bits (i.e., the
10 “probability of collision”) would be about 1 in 2 to the 29th power. Lachman and Farber dubbed their
11 content-based identifier a “True Name.”

12 17. Using a True Name, Lachman and Farber conceived various data structures and
13 methods for managing data (each data item correlated with a single True Name) within a network—
14 no matter the complexity of the data or the network. These data structures provide a key-map
15 organization, allowing for a rapid identification of any particular data item anywhere in a network by
16 comparing a True Name for the data item against other True Names for data items already in the
17 network. In operation, managing data using True Names allows a user to determine the location of
18 any data in a network, determine whether access is authorized, and to selectively provide access to
19 specific content not possible using the conventional naming arts.

20 18. On April 11, 1995, Lachman and Farber filed their patent application, describing these
21 and other ways in which content-based “True Names” elevated data-processing systems over
22 conventional file-naming systems. The first True Name patent issued on November 2, 1999. The last
23 of the Patents-in-Suit has expired, and the allegations herein are directed to the time period before
24 expiration of the last of the Patents-in-Suit.

25 19. PersonalWeb has successfully enforced its intellectual property rights against third
26 party infringers, and its enforcement of the Patents-In Suit is ongoing. This enforcement has resulted
27 in PersonalWeb obtaining settlements and granting non-exclusive licenses regarding the Patents-in-
28 Suit.

GENERAL BACKGROUND

2 20. A webpage is a type of document that is typically retrieved over the World Wide Web,
3 made viewable and formatted (rendered) by a web browser, and displayed electronically. A “webpage”
4 often refers to what is visible in a browser, but sometimes also refers to a computer file (“webpage”
5 file” or “webpage base file”), usually written in Hypertext Markup Language (“HTML”) or a
6 comparable markup language. Such HTML files typically include text, formatting, and references
7 (hyperlinks) to other web contents, such as style sheets, scripts, and images. Web contents referenced
8 in an HTML or similar file are also called “webpage assets” or “asset files” herein. The web browser
9 coordinates the retrieval of the various asset files of a webpage and renders the webpage for display
10 from the webpage base file and the asset files referenced in the webpage base file.

11 21. On the World Wide Web, hyperlinks generally include Uniform Resource Identifiers
12 ("URIs"), which each typically include an address of a server from which the asset file could be
13 retrieved (e.g., "www.website.com"), a "path" to the location of that asset file on that server (e.g.,
14 "/directory/"), and a filename (e.g., "filename.ext").

15 22. On the Internet, a web browser typically retrieves a webpage base file from a remote
16 web server and retrieves referenced asset files from the same or different servers. The web browser
17 retrieves a webpage base file and asset files by making a GET “request” to a web server using the
18 Hypertext Transfer Protocol (“HTTP”), an industry standard. The web server may respond to such a
19 request with a HTTP “response” that includes the requested web content.

20 23. A static webpage is delivered exactly as stored, as web content in the web server's file
21 system or memory. In contrast, a dynamic webpage is generated by a web server application, usually
22 driven by server-side software, upon receipt of a request from a browser (user). For example, a picture
23 of a building might be delivered as static content (a picture) whereas the latest traffic conditions may
24 be delivered dynamically based on real time traffic information.

25 24. The speed of a browser retrieving webpage base files and incorporated asset files can
26 be increased by the browser storing previously retrieved webpage base files and asset files in a browser
27 “cache” on the computer running the browser. If a browser’s user later requests a previously retrieved
28 webpage base file or requests a webpage that includes an asset file previously used by the browser in

1 rendering the same or a different webpage (for example, by reloading a webpage or visiting the same
2 webpage again), the browser may use the cached webpage base file or asset file rather than having to
3 download the same file repeatedly over the Internet again.

4 25. Two computers communicating over the Internet usually are not directly connected to
5 each other but rather interact via chains of network appliances and other computers (e.g., “switches”
6 and “intermediate” servers). Many intermediate servers have caches similar to and complementing
7 the browser cache that store webpage base files and assets that pass through that intermediate server.
8 If a browser or server requests a file from the intermediate server that is present in that intermediate
9 server’s cache, the intermediate server can use the content in its cache to respond to the request rather
10 than send the request upstream towards the web server from which the file initially originated (also
11 called the “origin server”).

12 26. Responses to HTTP requests may include header elements (control elements) and a
13 body (the “object” that was requested). Under HTTP, web servers can include a “cache-control”
14 header with a response including a webpage or asset file. A “cache-control” header includes one or
15 more directives that instruct browsers and intermediate server caches (“intermediate caches”) as to
16 whether and for how long the file (object) included in the response may be cached. HTTP also
17 provides for including other headers in responses that provide similar types of instructions to browsers
18 and intermediate caches. Collectively, these other headers and directives in a “cache-control” header
19 are referred to herein as “cache-control headers.”

20 27. Given that webpage content changes, sometimes rather quickly and regularly, a
21 problem that website owners face is effectively instructing a browser that is re-rendering a previously
22 cached webpage that one or more of its cached files for that webpage are no longer the correct and
23 authorized content (the content of those files has changed) and similarly reauthorizing the use of those
24 cached files whose content has not changed.

25 28. On one hand, website owners want to encourage the browsers that render their web
26 pages to use cached files so as to reduce the number of requests for these files that are being made to
27 their webpage servers. Therefore, they frequently will set cache-control headers that authorize the
28 browser to cache their webpage and asset files so they are on hand when the browser needs to render

1 that webpage again. On the other hand, website owners want the browsers to use the latest authorized
 2 files so that their users do not see the wrong content when viewing their webpage.
 3

4 **DEFENDANT'S BACKGROUND**

5 29. On information and belief, Defendant has operated a website located at twitch.tv, and
 6 has done so since before expiration of the last to expire of the Patents-in-Suit, which has operated to
 7 provide authorized webpage content to its users in the manner herein described.¹

8 30. On information and belief, Defendant's web servers utilized a system of notifications
 9 and authorizations to control the distribution of content, *e.g.*, what webpage content may be served
 10 from web servers and intermediate caches and what cached webpage content a browser is re-authorized
 11 to use to render Defendant's webpage(s).

12 31. On information and belief, Defendant's system and its associated method of providing
 13 webpage content, used "conditional" HTTP GET requests with If-None-Match headers and associated
 14 content-based ETag values for various webpage and/or asset files required to render various webpages
 15 of the Defendant.

16 32. On information and belief, Defendant's system and its associated method of providing
 17 webpage content, also inserted fingerprints generated based on the content of asset files into the
 18 filenames of asset files required to render various webpages of the Defendant.

19 33. On information and belief, Defendant's system and associated method used these
 20 ETags and fingerprints to instruct both the intermediate cache servers and the endpoint caches at
 21 browsers to verify whether they were still authorized to reuse the previously cached webpage base
 22 files of Defendant and to instruct them to obtain newly authorized content in rendering Defendant's
 23 webpage when that content had changed.

24 34. On information and belief, Defendant thereby reduced the bandwidth and computation
 25 required by its origin servers and any intermediate cache servers to field user requests to render
 26

27
 28 ¹ While the complaint is sometimes written in the present or present perfect tense, all specific
 allegations are directed to the system's operations and the method's performance in the relevant time
 period.

1 Defendant's webpages as those servers only need to serve files whose content has changed. On
2 information and belief, this has allowed for the efficient update of cached information only when such
3 content has changed, thereby reducing transaction overhead and bandwidth and allowing the
4 authorized content to be served from the nearest cache.

5 35. More particularly, on information and belief, each of Defendant's webpages included
6 a webpage base file (e.g., a main or initial HTML file) and one or more asset files referenced in the
7 webpage base file. On information and belief, the references in the webpage base file to the asset files
8 needed to render the webpage were typically Uniform Resource Identifiers ("URIs"), which each
9 typically included a filename, the address of a server from which the asset file could be retrieved, and
10 a "path" to the location of that asset file on that server.

11 36. On information and belief, Defendant's website used a web application framework to
12 develop and compile various webpages of the Defendant, including asset files that were used in
13 rendering the webpages, and to generate fingerprints of the contents of asset files when the webpages
14 were compiled. On information and belief, the fingerprint of individual asset files that were part of
15 the webpage's content were included in the respective filenames of the individual asset files. On
16 information and belief, the modified filenames were then used as part of the URI used to access the
17 individual asset files over the Internet. On information and belief, when an asset file's content was
18 changed, a new fingerprint was generated and included in the filename, its URI thus being changed
19 accordingly.

20 37. On information and belief, the asset file fingerprint was generated with a hash function
21 and used to identify content changes. Furthermore, on information and belief, asset file URIs (with
22 respective fingerprints) were included in webpage base files. On information and belief, static
23 webpage base files, if any, were recompiled when any URI of a referenced asset file was changed (due
24 to the fingerprint of the referenced asset file changing). Thus, a content change in an asset file for a
25 given webpage would result in a change to its fingerprint, its URI, and a subsequent change to the
26 content of any static webpage base files referencing that changed asset file for that webpage.

27 38. On information and belief, a dynamic webpage base file generated for a webpage of
28 Defendant webpages in response to one request from a user could be the same as it was when it was

1 generated in response to a prior request from that or another user. On information and belief, this
2 would not be the case if any of the asset files referenced in the webpage base file had changed between
3 the time of the two requests and the URIs of the changed assets included fingerprints as described
4 above.

5 39. On information and belief, when Defendant created a webpage base file for a webpage,
6 whether dynamic or static, that webpage base file included a sequence of bits and an associated ETag
7 value was generated by Defendant by applying a hash function to the sequence of bits; wherein any
8 two webpage base files comprising identical sequences of bits had identical associated ETag values.
9 Thus, on information and belief, when a webpage base file's content was changed and a new associated
10 ETag value was generated by Defendant, it thereafter instructed the respective service by intermediate
11 cache servers or use by endpoint caches such as browser caches to no longer use the previous webpage
12 base file's content.

13 40. On information and belief, when an intermediate cache server or a browser requested
14 a webpage from the Defendant for the first time, it sent an HTTP GET request with the webpage's
15 URI and Defendant's origin server or an upstream cache server responded by sending an HTTP 200
16 (OK) response message containing the webpage base file, along with its respective associated ETag.
17 On information and belief, the intermediate cache server or a browser then sent individual HTTP Get
18 requests, each with an asset URI that was referenced in the webpage base file, and Defendant's origin
19 server or an upstream cache server responded by sending individual HTTP 200 responses containing
20 the requested asset files, along with their respective associated ETags. On information and belief,
21 upon receipt of the HTTP 200 responses, the intermediate cache server or browser cached the webpage
22 and asset files with their associated URI and associated ETag values and the browser used them in
23 rendering the requested web page of the Defendant. On information and belief, the intermediate cache
24 servers and browser caches were caused to maintain databases/tables which mapped the URIs of
25 asset/webpage base files to their respective responses and, if applicable, associated cache-control
26 headers and ETags.

27 41. On information and belief, by responding to an HTTP GET request for a given webpage
28 by transmitting content of a webpage/asset file with an associated ETag, Defendant instructed the

1 browser cache and all intermediate cache servers, to use an HTTP conditional GET request the next
2 time that webpage/asset file is requested. More specifically, on information and belief, the browser or
3 intermediate cache is instructed to include the ETag in the HTTP conditional GET request with an “If-
4 None-Match” header to re-verify that they are still authorized to serve or use that content or determine
5 that they are no longer authorized to use that content and therefore must use new content.

6 42. On information and belief, Defendant did this, for example, by causing cache-control
7 headers to be included in HTTP responses containing its webpage/asset files. On information and
8 belief, Defendant benefits from using the ETags to control the distribution of its webpage content by
9 communicating to a downstream cache and to a browser which of Defendant’s cached webpage base
10 files it is reauthorized to serve/use and what newly authorized files it must first obtain in
11 serving/rendering Defendant’s webpages.

12 43. More particularly, on information and belief, when a browser again requested the
13 Defendant’s webpage, the browser, based on the cache-control headers received in the original
14 response, sent a conditional GET request with an If-None-Match header using the associated ETag
15 value and the URI for the webpage base file so as to be notified whether the browser still had
16 Defendant’s authority to render the webpage with its locally cached webpage base file.

17 44. On information and belief, under most circumstances, a responding intermediate cache
18 server, having an ETag for that URI responded to the request by determining whether it had the same
19 associated ETag value in its list of associated ETag values for that URI. If it had no ETag value for
20 that URI, the request was passed up to an upstream intermediate cache server capable of responding
21 or, if none, to the Defendant’s origin server which performed the response.

22 45. On information and belief, if the responding server had the webpage content for that
23 URI and there was a match between the ETag it received in the request with the ETag it currently had
24 associated for that URI, it sent back an HTTP 304 (Not Modified) response message; this message
25 notifying the browser that the same webpage content was present at the responding server and that the
26 browser was still authorized to use that previously cached webpage base file to render the webpage.
27 On information and belief, upon receipt of the HTTP 304 response, the browser accessed the locally
28 cached webpage base file in rendering the webpage.

1 46. On information and belief, if the webpage base file's associated ETag sent by the
2 browser in the conditional GET If-None-Match request did not match the associated ETag maintained
3 at the responding server (or other intermediate cache servers further upstream or the origin server) for
4 that URI, the responding server sent back an HTTP 200 response along with the new webpage base
5 file and its new ETag value. The HTTP 200 response indicated to the browser that it was not
6 authorized to use (or serve, in the case of an intermediate cache server receiving the HTTP 200
7 response) the previously cached webpage base file. In response to receiving the HTTP 200 response,
8 the browser (or intermediate cache server) was instructed to update its respective cache with the new
9 webpage base file and associated ETag. The browser subsequently read the new webpage base file
10 and the asset file URIs contained therein to render the webpage.

11 47. On information and belief, for a particular asset file URI in the webpage base file for
12 which there was a matching entry in the browser's cache and that cache entry did not include an
13 associated ETag value, the browser was allowed to use the cached content of the previously received
14 asset file, subject to the asset file's cache-control headers. On information and belief, if the cache-
15 control headers did not allow the cached asset file content to be re-used or if there was no entry in the
16 browser's cache for the asset file's URI, the browser sent an HTTP GET request with the asset file's
17 URI; and the responding intermediate or origin server responded to the GET request by sending the
18 asset file for that URI and, if any, the corresponding cache-control headers and/or associated ETag
19 with an HTTP 200 response. On information and belief, in response to receiving the HTTP 200
20 response, the browser cached the asset file, if any, and its cache-control headers and/or associated
21 ETag and used the newly received asset files in rendering Defendant's webpage. On information and
22 belief, if the downstream intermediate cache or the browser was later required to again serve or render
23 the webpage, it went through the above process to determine which file content it still had authority
24 to access or whether it needed to access different authorized content to serve or render the webpage
25 via the HTTP 304 and HTTP 200 responses.

26 48. On information and belief, the browser repeated this process for various asset files for
27 which it had an associated ETag value and asset files with URIs in the webpage base file.

49. On information and belief, in this manner, Defendant used (1) ETag values and (2) asset files referenced by URIs with fingerprints based on the asset files' content to control the behavior of downstream intermediate cache servers and endpoint caches to assure that they only accessed and used Defendant's latest authorized webpage content to serve or to render its webpages.

FIRST CLAIM FOR RELIEF

INFRINGEMENT OF U.S. PATENT NO. 6,928,442

50. PersonalWeb repeats and realleges paragraphs 1-49, as if the same were fully stated herein.

51. On August 9, 2005, United States Patent No. 6,928,442 (the “‘442 patent”) was duly and legally issued for an invention entitled “Enforcement and Policing of Licensed Content Using Content-Based Identifiers.” PersonalWeb has an ownership interest in the ‘442 patent by assignment, including the exclusive right to enforce the ‘442 patent within the PersonalWeb Patent Field, and continues to hold that ownership interest in the ‘442 patent.

52. Defendant has infringed at least claims 10 and 11 of the '442 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '442 patent pursuant to 35 U.S.C. § 271.

53. For example, claim 10 covers “a method, in a system in which a plurality of files are distributed across a plurality of computers.” On information and belief, Defendant has used a system of notifications and authorizations to distribute a plurality of files, *e.g.*, Defendant’s files containing content necessary to render its webpages, across a plurality of computers such as production servers, origin servers, intermediate cache servers and endpoint caches used by browsers rendering Defendant’s webpages.

54. Claim 10 then recites the act of “obtaining a name for a data file, the name being based at least in part on a given function of the data, wherein the data used by the function comprises the contents of the particular file.” As set forth above, on information and belief, Defendant generated or

1 otherwise obtained ETags for its webpage and asset files used to render its webpages using a hash
2 function, wherein the ETags were based on the contents of the particular files. Moreover, Defendant
3 caused the intermediate caches servers and endpoint caches to obtain the ETags in HTTP 200
4 responses sent from Defendant's origin servers. On information and belief, Defendant caused
5 intermediate cache servers and its origin servers to obtain ETags in conditional GET messages from
6 endpoint and intermediate caches, as described *supra*.

7 55. Claim 10 then recites the act of "determining, using at least the name, whether a copy
8 of the data file is present on at least one of said computers." On information and belief, as set forth
9 above, Defendant has caused its origin servers and the intermediate cache servers between an endpoint
10 cache and one of its origin servers to, in response to receiving a conditional GET request with an If-
11 None-Match header, determine whether it has a file present that matches the URI in the conditional
12 GET and to compare the ETag in the conditional GET to the ETag for that URI and determine whether
13 a copy of the content having that ETag is present.

14 56. Claim 10 then recites the act of "determining whether a copy of the data file that is
15 present on at least one of said computers is an unauthorized copy or an unlicensed copy of the data
16 file." On information and belief, as set forth above, if there was a match, the origin or intermediate
17 cache server determined that the copy of the file present at the downstream intermediate cache server
18 and/or the endpoint cache was an authorized or licensed copy of the data file. Conversely, if there was
19 no match, it determined that the copy of the file present at the downstream intermediate cache server
20 and/or the endpoint cache was an unauthorized copy of the data file. Likewise, if the browser
21 determined that it had a file with a matching URI, the browser determined that it was still authorized
22 to use that file.

23 57. Defendant's acts of infringement caused damage to PersonalWeb and PersonalWeb is
24 entitled to recover from Defendant the damages sustained by PersonalWeb as a result of Defendant's
25 wrongful acts in an amount subject to proof at trial.

26
27
28

SECOND CLAIM FOR RELIEF

INFRINGEMENT OF U.S. PATENT NO. 7,802,310

58. PersonalWeb repeats and realleges paragraphs 1–49, as if the same were fully stated herein.

59. On September 21, 2010, United States Patent No. 7,802,310 (the “310 patent”) was duly and legally issued for an invention entitled “Controlling Access to Data in a Data Processing System.” PersonalWeb has an ownership interest in the ’310 patent by assignment, including the exclusive right to enforce the ’310 patent within the PersonalWeb Patent Field, and continues to hold that ownership interest in the ’310 patent.

60. Defendant has infringed at least claims 20 and 69 of the '310 patent by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the distribution of its webpage content in the manner described herein. Defendant's infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '310 patent pursuant to 35 U.S.C. § 271.

61. For example, claim 20 covers a “computer-implemented method operable in a system which includes a plurality of computers.” On information and belief, Defendant used the claimed computer implemented method by using a system of notifications and authorizations to control the distribution of data items, such as various webpage and asset files, necessary to render its webpages, across a plurality of computers such as production servers, origin servers, intermediate cache servers, and endpoint caches.

62. Claim 20 then recites “controlling distribution of content from a first computer to at least one other computer, in response to a request obtained by a first device in the system from a second device in the system, the first device comprising hardware including at least one processor, the request including at least a content-dependent name of a particular data item, the content-dependent name being based at least in part on a function of at least some of the data comprising the particular data item, wherein the function comprises a message digest function or a hash function, and wherein two identical data items will have the same content-dependent name.” On information and belief, as set forth above, Defendant has caused downstream intermediate cache servers and endpoint caches to

1 send conditional GET requests with If-None-Match headers containing ETags that are fielded by
2 upstream cache or origin servers. On information and belief, the ETags were content-dependent names
3 for a data item based on hashing the data item's contents; and when the file's content changed a new
4 content-dependent name was determined. On information and belief, in Defendant's method, a first
5 computer, such as the intermediate cache server or origin server, received such conditional GET
6 requests from a second computer, such as a user browser or other intermediate cache server, regarding
7 data items, such as webpage or asset files, the requests including ETags associated with the respective
8 data items.

9 63. Claim 20 then recites "based at least in part on said content-dependent name of said
10 particular data item, the first device (A) permitting the content to be provided to or accessed by the at
11 least one other computer if it is not determined that the content is unauthorized or unlicensed,
12 otherwise, (B) if it is determined that the content is unauthorized or unlicensed, not permitting the
13 content to be provided to or accessed by the at least one other computer." On information and belief,
14 the first computer, such as an upstream intermediate cache server or origin server, maintained a
15 plurality of ETags associated with Defendant's asset and webpage base files. On information and
16 belief, the ETag in a request and the ETag maintained by the first computer for the particular data item
17 sought by the request were compared to determine whether the associated content present at the
18 downstream computer was still authorized to be used/served or whether new authorized content must
19 be provided thereto. If it was determined that the data item corresponding to the received ETag was
20 still authorized to be used, the first computer sent back an HTTP 304 response authorizing the
21 downstream cache server or end-user cache to access the file content already present in order to serve
22 it or to use it to render the webpage. On information and belief, if it had been determined that the data
23 item corresponding to received E-tag was no longer authorized, the first computer sent back an HTTP
24 200 response which indicated to the downstream cache server or end-user cache that was not
25 authorized to access the old content and must access the new authorized file content contained in the
26 HTTP 200 response to serve it or to use it to render the webpage.

27 64. For further example, claim 69 covers a "system operable in a network of computers,
28 the system comprising hardware including at least a processor, and software, in combination with said

1 hardware.” On information and belief, Defendant has controlled the distribution of its website content
2 across a system that included a network of computers, such as its production servers as well as origin
3 servers, intermediate cache servers, and endpoint caches, all comprising hardware including a
4 processor. On information and belief, Defendant has utilized software, in combination with such
5 hardware, such as a web development framework, software utilized in implementing the HTTP web
6 protocol, and software used on host servers that Defendant used to serve its content.

7 65. Claim 69 then recites the system “(a) to receive at a first computer, from a second
8 computer, a request regarding a data item, said request including at least a content-dependent name
9 for the data item, the content-dependent name being based at least in part on a function of the data in
10 the data item, wherein the data used by the function to determine the content-dependent name
11 comprises at least some of the contents of the data item, wherein the function that was used is a
12 message digest function or a hash function, and wherein two identical data items will have the same
13 content-dependent name.” On information and belief, as set forth above, Defendant has caused
14 downstream intermediate cache servers and endpoint caches to send conditional GET requests with
15 URIs including fingerprints that are fielded by upstream cache or origin servers. On information and
16 belief, the URIs including fingerprints were content-dependent names for a data item calculated by
17 hashing the file’s contents; and when the file’s content changed a new content-dependent name was
18 determined. On information and belief, in Defendant’s system, a first computer, such as the
19 intermediate cache server or origin server, received such conditional GET requests from a second
20 computer, such as a user browser, regarding data items, such as asset files, using content-dependent
21 names such as URIs including fingerprints associated with the data items.

22 66. Claim 69 then recites “(b) in response to said request: (i) to cause the content-dependent
23 name of the data item to be compared to a plurality of values; and (ii) to determine if access to the data
24 item is authorized or unauthorized based on whether or not the content-dependent name corresponds
25 to at least one of said plurality of values, and (iii) based on whether or not it is determined that access
26 to the data item is authorized or unauthorized, to allow the data item to be provided to or accessed by
27 the second computer if it is not determined that access to the data item is unauthorized.” On
28 information and belief, the first computer, such as an upstream intermediate cache server or origin

1 server, maintained a plurality of URI values associated with Defendant's asset and webpage base files;
2 compared the URI value received in a conditional GET request from the second (downstream)
3 computer to that plurality of URI values; that comparison allowed the first computer to determine
4 whether the content-dependent name in the request corresponded to one of the plurality of stored URI
5 values and to determine whether access to the data item was still authorized or not. On information
6 and belief, in particular when there was a match, the first computer determined the associated content
7 present at the downstream computer was still authorized to be used/served or whether new authorized
8 content must be provided thereto. If it was determined that the data item corresponding to the received
9 URI including a fingerprint was still authorized to be used, the first computer has sent back an HTTP
10 304 response authorizing the downstream cache server or end-user cache to access the file content
11 already present in order to serve it or to use it to render the webpage.

12 67. Defendant's acts of infringement have caused damage to PersonalWeb and
13 PersonalWeb is entitled to recover from Defendant the damages sustained by PersonalWeb as a result
14 of Defendant's wrongful acts in an amount subject to proof at trial.

15

16 **THIRD CLAIM FOR RELIEF**

17 **INFRINGEMENT OF U.S. PATENT NO. 7,945,544**

18 68. PersonalWeb repeats and realleges paragraphs 1–49, as if the same were fully stated
19 herein.

20 69. On May 17, 2011, United States Patent No. 7,945,544 (the "'544 patent") was duly and
21 legally issued for an invention entitled "Similarity-Based Access Control of Data in a Data Processing
22 System." PersonalWeb has an ownership interest in the '544 patent by assignment, including the
23 exclusive right to enforce the '544 patent within the PersonalWeb Patent Field, and continues to hold
24 that ownership interest in the '544 patent.

25 70. Defendant has infringed at least claims 46, 48, 52, and 55 of the '544 patent by its
26 manufacture, use, sale, importation, and/or offer for sale of products or services, and/or controlling the
27 distribution of its webpage content in the manner described herein. Defendant's infringement is literal

1 and/or under the doctrine of equivalents and Defendant is liable for its infringement of the '544 patent
 2 pursuant to 35 U.S.C. § 271.

3 71. For example, claim 46 covers a claimed “computer-implemented method.” On
 4 information and belief, Defendant uses the claimed computer implemented method by using a system
 5 of notifications and authorizations to locate and control the distribution of data items, such as various
 6 webpage and asset files, necessary to render its webpages.

7 72. Claim 46 then recites the act of “(A) for each particular file of a plurality of files:
 8 (a2) determining a particular digital key for the particular file, wherein the particular file comprises a
 9 first one or more parts.” On information and belief, each of Defendant’s webpages comprises one or
 10 more asset files and has an associated webpage base file, the webpage base file containing the URIs
 11 having fingerprints of a plurality of asset files comprising the webpage, and once the webpage and
 12 asset files are compiled and complete, Defendant stores them on a host system. On information and
 13 belief, the webpage base file’s associated ETag value is generated by applying a hash algorithm to the
 14 webpage base file’s contents. On information and belief, whenever a new webpage base file is
 15 generated or the webpage base file’s content changes, Defendant caused an ETag to be determined
 16 and associated to the webpage base file.

17 73. Claim 46 then recites “each part of said first one or more parts having a corresponding
 18 part value, the part value of each specific part of said first one or more parts being based on a first
 19 function of the contents of the specific part, wherein two identical parts will have the same part value
 20 as determined by the first function, and wherein the particular digital key for the particular file is
 21 determined using a second function of the one or more of part values of said first one or more parts.”
 22 On information and belief, prior to various asset files being stored on a host system, a fingerprint is
 23 generated for each of these asset files by applying a hash function to the asset file’s contents and the
 24 fingerprints are inserted into the URIs for the respective asset files. On information and belief, the
 25 webpage’s ETag value is generated by applying a second hash function to the webpage base file’s
 26 contents, which include the URIs of one or more of the asset files which comprise the webpage’s
 27 contents. On information and belief, because the respective asset files’ URIs include the fingerprints
 28 of their content, the webpage’s ETag value will change and a new associated ETag value is generated

1 to represent the webpage's content, when the content changes and two identical webpages having the
 2 identical content represented by their webpage base file will have the same ETag value.

3 74. Claim 46 then recites the act of "(a2) adding the particular digital key of the particular
 4 file to a database, the database including a mapping from digital keys of files to information about the
 5 corresponding files." On information and belief, Defendant caused the origin server, intermediate
 6 caches and browser caches to maintain databases/tables which mapped the ETag of each webpage's
 7 webpage base file to its URI, and information about the corresponding webpage, such as, for example,
 8 information from cache-control headers for the webpage.

9 75. Claim 46 then recites "(B) determining a search key based on search criteria, wherein
 10 the search criteria comprise a second one or more parts, each of said second one or more parts of said
 11 search criteria having a corresponding part value, the part value of each specific part of said second
 12 one or more parts being based on the first function of the contents of the specific part, and wherein the
 13 search key is determined using the second function of the one or more of part values of said second
 14 one or more parts." On information and belief, when a downstream intermediate cache server or a
 15 browser again requested a webpage of Defendant, Defendant caused it to send a conditional GET
 16 request with an If-None-Match header with the webpage's associated ETag value. On information
 17 and belief, the received ETag value was determined using the second hash function of the webpage's
 18 webpage base file, which included URIs including fingerprints for one or more of the asset files which
 19 comprised the webpage's contents.

20 76. Claim 46 then recites "(C) attempting to match the search key with a digital key in the
 21 database." On information and belief, when the responding server received the webpage's ETag value
 22 in a conditional GET request with an If-None-Match header, it compared the received ETag with the
 23 ETag it has maintained in a database/table corresponding to the URI of the webpage's webpage base
 24 file to determine if there is matching value for that webpage.

25 77. Claim 46 then recites "(D) if the search key matches a particular digital key in the
 26 database, providing information about the file corresponding to the particular digital key." On
 27 information and belief, if the responding server had a matching ETag value for the webpage's webpage
 28 base file, the responding server sent an HTTP 304 response, which included information about the

1 corresponding webpage, such as, for example, information from cache-control headers for the
2 webpage.

3 78. Defendant's acts of infringement have caused damage to PersonalWeb and
4 PersonalWeb is entitled to recover from Defendant the damages sustained by PersonalWeb as a result
5 of Defendant's wrongful acts in an amount subject to proof at trial.

6

7 **FOURTH CLAIM FOR RELIEF**

8 **INFRINGEMENT OF U.S. PATENT NO. 8,099,420**

9 79. PersonalWeb repeats and realleges paragraphs 1–49, as if the same were fully stated
10 herein.

11 80. On January 17, 2012, United States Patent No. 8,099,420 (the “420 patent”) was duly
12 and legally issued for an invention entitled “Accessing Data in a Data Processing System.”
13 PersonalWeb has an ownership interest in the ’420 patent by assignment, including the exclusive right
14 to enforce the ’420 patent within the PersonalWeb Patent Field, and continues to hold that ownership
15 interest in the ’420 patent.

16 81. Defendant has infringed claims 25, 26, 27, 29, 30, 32, 34–36, and 166 of the ’420 patent
17 by its manufacture, use, sale, importation, and/or offer for sale of products or services, and/or
18 controlling the distribution of its webpage content in the manner recited herein. Defendant's
19 infringement is literal and/or under the doctrine of equivalents and Defendant is liable for its
20 infringement of the ’420 patent pursuant to 35 U.S.C. § 271.

21 82. For example, claim 166 covers a “system comprising hardware, including at least a
22 processor, and software, in combination with said hardware.” On information and belief, Defendant
23 has controlled the distribution of its website content across a system that included hardware including
24 a processor, such as its production servers as well as origin servers, intermediate cache servers, and
25 endpoint caches; and software, in combination with such hardware, such as a web development
26 framework, software utilized in implementing the HTTP web protocol, and the software used on host
27 servers that Defendant used to serve its webpages.

1 83. Claim 166 then recites “(A) for a particular data item in a set of data items, said
 2 particular data item comprising a corresponding particular sequence of bits.” On information and
 3 belief, Defendant’s system has controlled the distribution of asset files and webpage base files
 4 necessary to render its webpages which represent particular data items, and each of these files comprise
 5 a corresponding sequence of bits.

6 84. Claim 166 then recites that for the particular data item to “(a1) determine one or more
 7 content-dependent digital identifiers for said particular data item, each said content-dependent digital
 8 identifier being based at least in part on a given function of at least some of the bits in the particular
 9 sequence of bits of the particular data item, wherein two identical data items will have the same digital
 10 identifiers as determined using said given function.” On information and belief, Defendant’s system
 11 has applied hash functions to each of various Defendant’s webpage base files to all of the bits of the
 12 file’s content to determine a fingerprint, an ETag, or both for the file’s content; whereby two identical
 13 data items have the same ETag values and the same fingerprint values. On information and belief,
 14 fingerprints were included in files’ URI and ETag values were associated with files’ URIs.

15 85. Claim 166 then recites that for the particular data item “(a2) selectively permits the
 16 particular data item to be made available for access and to be provided to or accessed by or from at
 17 least some of the computers in a network of computers, wherein the data item is not to be made
 18 available for access or provided without authorization, as resolved based, at least in part, on whether
 19 or not at least one of said one or more content-dependent digital identifiers for said particular data item
 20 corresponds to an entry in one or more databases, each of said one or more databases comprising a
 21 plurality of identifiers, each of said identifiers in each said database corresponding to at least one data
 22 item of a plurality of data items, and each of said identifiers in each said database being based, at least
 23 in part, on at least some of the data in a corresponding data item.”

24 86. On information and belief, Defendant’s system has included one or more web servers
 25 with databases containing ETag values associated with the URIs for various of the asset and webpage
 26 base files necessary to render its webpages; moreover, Defendant’s system has used a system of
 27 conditional GET requests with If-None-Match headers and HTTP 304 and HTTP 200 responses
 28 containing the ETags, as described more particularly *supra*, to ensure that downstream caches only

1 access authorized file content to either serve that file content further downstream or to use it to render
2 Defendant’s webpages. On information and belief, in particular, as more fully described *supra*, the
3 system compared the ETag received in a given conditional GET request with the ETags contained in
4 the database to selectively determine whether the requesting computer could access the file content it
5 already had or must access newly received authorized content.

6 87. Defendant's acts of infringement have caused damage to PersonalWeb and
7 PersonalWeb is entitled to recover from Defendant the damages sustained by PersonalWeb as a result
8 of Defendant's wrongful acts in an amount subject to proof at trial.

PRAYER FOR RELIEF

11 WHEREFORE, Plaintiff PersonalWeb requests entry of judgment in its favor and against
12 Defendant as follows:

13 a) Declaration that Defendant has infringed U.S. Patent Nos. 6,928,442, 7,802,310,
14 7,945,544, and 8,099,420 as described in this action;

15 b) Awarding the damages arising out of Defendant's infringement of U.S. Patent Nos.
16 6,928,442, 7,802,310, 7,945,544, and 8,099,420, together with pre-judgment and post-judgment
17 interest, in an amount according to proof;

18 c) An award of attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise permitted by
19 law; and

20 d) For costs incurred and such other and further relief as the Court may deem just and
21 proper.

22 || Respectfully submitted,

23 | Dated: September 13, 2018

STUBBS, ALDERTON & MARKILES, LLP

By: */s/ Michael A. Sherman*

Michael A. Sherman

Jeffrey F. Gersh

Sandeep Seth

Wesley W. Monroe

Stanley H. Thompson, Jr.

Viviana Boero Hedrick

Attorneys for Plaintiffs

1 Dated: September 13, 2018

MACEIKO IP

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

By: /s/ Theodore S. Maceiko

Theodore S. Maceiko (SBN 150211)

ted@maceikoip.com

MACEIKO IP

420 2nd Street

Manhattan Beach, California 90266

Telephone: (310) 545-3311

Facsimile: (310) 545-3344

Attorneys for Plaintiff

PERSONALWEB TECHNOLOGIES, LLC,

Dated: September 13, 2018

DAVID D. WIER

By: /s/ David D. Wier

David D. Wier

david.wier@level3.com

Vice President and Assistant General Counsel

Level 3 Communications, LLC

1025 Eldorado Boulevard

Broomfield, CO 80021

Telephone: (720) 888-3539

Attorneys for Plaintiff

LEVEL 3 COMMUNICATIONS, LLC

DEMAND FOR JURY TRIAL

2 Pursuant to Fed. R. Civ. P. 38(b) and Local Rule 3-6, Plaintiff PersonalWeb Technologies,
3 LLC hereby demands a trial by jury on all issues triable in this action.

4 || Respectfully submitted,

5 || Dated: September 13, 2018

STUBBS, ALDERTON & MARKILES, LLP

By: /s/ Michael A. Sherman

Michael A. Sherman
Jeffrey F. Gersh
Sandeep Seth
Wesley W. Monroe
Stanley H. Thompson, Jr.
Viviana Boero Hedrick
Attorneys for Plaintiffs

¶ Dated: September 13, 2018

MACEIKO IP

By: /s/ *Theodore S. Maceiko*

Theodore S. Maceiko (SBN 150211)
ted@maceikoip.com
MACEIKO IP
420 2nd Street
Manhattan Beach, California 90266
Telephone: (310) 545-3311
Facsimile: (310) 545-3344
Attorneys for Plaintiff
PERSONALWEB TECHNOLOGIES, LLC,

Dated: September 13, 2018

DAVID D. WIER

By: /s/ *David D. Wier*

David D. Wier
david.wier@level3.com
Vice President and Assistant General Counsel
Level 3 Communications, LLC
1025 Eldorado Boulevard
Broomfield, CO 80021
Telephone: (720) 888-3539
Attorneys for Plaintiff
LEVEL 3 COMMUNICATIONS, LLC